The New York Times | https://nyti.ms/10oJH3d

Opinion | OP-ED COLUMNIST

Living With the Surveillance State

Bill Keller JUNE 16, 2013

MY colleague Thomas Friedman's levelheaded take on the National Security Agency eavesdropping uproar needs no boost from me. His column soared to the top of the "most e-mailed" list and gathered a huge and mostly thoughtful galaxy of reader comments. Judging from the latest opinion polling, it also reflected the prevailing mood of the electorate. It reflected mine. But this is a discussion worth prolonging, with vigilant attention to real dangers answering overblown rhetoric about theoretical ones.

Tom's important point was that the gravest threat to our civil liberties is not the N.S.A. but another 9/11-scale catastrophe that could leave a panicky public willing to ratchet up the security state, even beyond the war-on-terror excesses that followed the last big attack. Reluctantly, he concludes that a well-regulated program to use technology in defense of liberty — even if it gives us the creeps — is a price we pay to avoid a much higher price, the shutdown of the world's most open society. Hold onto that qualifier: "well regulated."

The N.S.A. data-mining is part of something much larger. On many fronts, we are adjusting to life in a surveillance state, relinquishing bits of privacy in exchange for the promise of other rewards. We have a vague feeling of uneasiness about these transactions, but it rarely translates into serious thinking about where we set the limits.

Exhibit A: In last Thursday's Times Joseph Goldstein reported that local law enforcement agencies, "largely under the radar," are amassing their own DNA databanks, and they often do not play by the rules laid down for the databases compiled by the F.B.I. and state crime labs. As a society, we have accepted DNA evidence as a reliable tool both for bringing the guilty to justice and for exonerating the wrongly accused. But do we want police agencies to have complete license — say, to sample our DNA surreptitiously, or to collect DNA from people not accused of any wrongdoing, or to share our most private biological information? Barry Scheck, co-director of the Innocence Project and a member of the New York State Commission on Forensic Science, says regulators have been slow to respond to what he calls rogue databanks. And a recent Supreme Court ruling that defined DNA-gathering as a legitimate police practice comparable to fingerprinting is likely to encourage more freelancing. Scheck says his fear is that misuse will arouse public fears of government overreach and discredit one of the most valuable tools in our justice system. "If you ask the American people, do you support using DNA to catch criminals and exonerate the innocent, everybody says yes," Scheck told me. "If you ask, do you trust the government to have your DNA, everybody says no."

Exhibit B: Nothing quite says Big Brother like closed-circuit TV. In Orwell's Britain, which is probably the democratic world's leading practitioner of CCTV monitoring, the omnipresent pole-mounted cameras are being supplemented in some jurisdictions by wearable, night-vision cop-cams that police use to record every drunken driver, domestic violence call and restive crowd they encounter. New York last year joined with Microsoft to introduce the eerily named Domain Awareness System, which connects 3,000 CCTV cameras (and license-plate scanners and radiation detectors) around the city and allows police to cross-reference databases of stolen cars, wanted criminals and suspected terrorists. Fans of TV thrillers like "Homeland,""24" and the British series "MI-5" (guilty, guilty and guilty) have come to think of the omnipresent camera as a crime-fighting godsend. But who watches the watchers? Announcing the New York system, the city assured us that no one would be monitored because of race, religion, citizenship status, political affiliation, etc., to which one skeptic replied, "But we've

heard that one before."

Exhibit C: Congress has told the F.A.A. to set rules for the use of spy drones in American air space by 2015. It is easy to imagine the value of this next frontier in surveillance: monitoring forest fires, chasing armed fugitives, search-and-rescue operations. Predator drones already patrol our Southern border for illegal immigrants and drug smugglers. Indeed, border surveillance may be critical in persuading Congress to pass immigration reform that would extend our precious liberty to millions living in the shadows. I for one would count that a fair trade. But where does it stop? Scientific American editorialized in March: "Privacy advocates rightly worry that drones, equipped with high-resolution video cameras, infrared detectors and even facial-recognition software, will let snoops into realms that have long been considered private." Like your backyard. Or, with the sort of thermal imaging used to catch the Boston bombing fugitive hiding under a boat tarp, your bedroom.

And then there is the Internet. We seem pretty much at peace, verging on complacent, about the exploitation of our data for commercial, medical and scientific purposes — as trivial as the advertising algorithm that pitches us camping gear because we searched the Web for wilderness travel, as valuable as the digital record-sharing that makes sure all our doctors know what meds we're on.

In an online debate about the N.S.A. eavesdropping story the other day, Eric Posner, a professor at the University of Chicago Law School, pointed out that we have grown comfortable with the Internal Revenue Service knowing our finances, employees of government hospitals knowing our medical histories, and public-school teachers knowing the abilities and personalities of our children.

"The information vacuumed up by the N.S.A. was already available to faceless bureaucrats in phone and Internet companies — not government employees but strangers just the same," Posner added. "Many people write as though we make some great sacrifice by disclosing private information to others, but it is in fact simply the way that we obtain services we want — whether the market services of doctors, insurance companies, Internet service providers, employers, therapists

and the rest or the nonmarket services of the government like welfare and security."

Privacy advocates will retort that we surrender this information wittingly, but in reality most of us just let it slip away. We don't pay much attention to privacy settings or the "terms of service" fine print. Our two most common passwords are "password" and "123456."

From time to time we get worrisome evidence of data malfeasance, such as the last big revelation of N.S.A. eavesdropping, in 2005, which disclosed that the agency was tapping Americans without the legal nicety of a warrant, or the more recent I.R.S. targeting of right-wing political groups. But in most cases the advantages of intrusive technology are tangible and the abuses are largely potential. Edward Snowden's leaks about N.S.A. data-mining have, so far, not included evidence of any specific abuse.

The danger, it seems to me, is not surveillance per se. We have already decided, most of us, that life on the grid entails a certain amount of intrusion. Nor is the danger secrecy, which, as Posner notes, "is ubiquitous in a range of uncontroversial settings," a promise the government makes to protect "taxpayers, inventors, whistle-blowers, informers, hospital patients, foreign diplomats, entrepreneurs, contractors, data suppliers and many others."

The danger is the absence of rigorous, independent regulation and vigilant oversight to keep potential abuses of power from becoming a real menace to our freedom. The founders created a system of checks and balances, but the safeguards have not kept up with technology. Instead, we have an executive branch in a leak-hunting frenzy, a Congress that treats oversight as a form of partisan combat, a political climate that has made "regulation" an expletive and a public that feels a generalized, impotent uneasiness. I don't think we're on a slippery slope to a police state, but I think if we are too complacent about our civil liberties we could wake up one day and find them gone — not in a flash of nuclear terror but in a gradual, incremental surrender.

A version of this op-ed appears in print on June 17, 2013, on Page A17 of the New York edition with the

headline: Living With the Surveillance State.